UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/092,973	03/07/2002	Jean-Claude Junqua	9432-000148	1465

27572 7590 03/28/2006

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. BOX 828
BLOOMFIELD HILLS, MI 48303

EXAMINER	
EDOUARD, PATRICK NESTOR	
ART UNIT	**PAPER NUMBER**
2626	

DATE MAILED: 03/28/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/092,973	JUNQUA, JEAN-CLAUDE	
	Examiner	Art Unit	
	Minerva Rivero	2655	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 November 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 11/21/05 has been entered.

Response to Amendment

2. In the Remarks submitted 11/21/05, Applicants amended claims 1, 21, and 28, added claim 30, and submitted arguments for allowability of pending claims.

Response to Arguments

1. Applicant's arguments with respect to claims 1-15, 16-26 and 28-29 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-15, 17-20 and 28-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Traynor (US 2002/0007278), in view of Carter *et al.* ("An Integrated Biometric Database", IEE Colloquium on Electronic Images and Image Processing in Security and Forensic Sciences, IEE (1990)).

Regarding claims 1 and 28, Traynor discloses an apparatus for and method of interacting with a secure resource accessible through a telephone system of the type that provides telephone access through a plurality of extensions, comprising:

a security server having an interface for sending messages to said telephone system, said messages being adapted to provide control signals to said secure resource (*web server* and *secure transactions*, [0019], Lines 1-4; Fig. 1, elements 110 and 120; *authenticating the voice of the caller*, [0010], Lines 4-7);

a biometric data store that stores biometric data associated with at least one user (*database contains information for each caller*, [0019], Lines 1-4; *information includes the callers voice print*, [0019], Lines 8-9);

a biometric data input system coupled to said security server and operable to obtain an utterance from said user (*callers transmit voice through callers' network and a voice profile for each caller is developed,* [0018]); and

a biometric verification/identification system being configured to generate a first confidence level based on a text independent component of said utterance, to access said data store, to evaluate said text independent component of said utterance vis-à-vis said stored biometric data, and to provide instructions to said security server and thereby provide control signals for interacting with said secure resource (*application verifies caller's voice*, [0015], Lines 19-22; *voice profile will be used for voice verification*, [0018], Lines 10-11; *voice profile is coupled with caller's own pin number (two verification levels)*, [0018], Lines 12-13; *uses involving remote voice control of a system*, [0016], Lines 1-4).

However, Traynor does not disclose but Carter *et al.* do disclose said verification/identification system is adapted to access a data structure storing associations among different types of biometric data and individual one of said extensions in order to retrieve stored biometric data associated with an extension being operated by a user (*see Integrated Database Overview, each subject record includes a voice recording, a signature record and a face image,* Page 2, 3rd Paragraph, Lines 1-8 and 12-22).

Therefore it would have been obvious to one ordinarily skilled in the art at the time of the invention to supplement the teachings of Traynor, by having said verification/identification system be adapted to access a data structure storing

associations among different types of biometric data associated and individual one of said extensions in order to retrieve stored biometric data associated with an extension being operated by a user, as taught by Carter *et al.*, in order to effectively retrieve the complete biometric record that corresponds to a particular user.

4. Regarding claim 2, Traynor teaches a telephone network (Fig. 1, element 200), thus it has an inherent telephony interface coupled to said telephone system.

5. Regarding claim 3, Traynor discloses said interface is an interface coupling said security server with an intermediate system that in turn communicates with said telephone system (*speech recognition server*, Fig. 1, element 110).

6. Regarding claim 4, Traynor discloses said interface is a network interface for communicating messages over a network between said security server and said telephone system (*wireline and wireless networks*, Fig. 1, element 200).

7. Regarding claims 5, Traynor discloses said data store is configured to store biometric data in association with at least one of said plurality of extensions (*caller uses a wireless phone or wired telephone to enroll a voice profile* and *a voice profile is developed*, [0018], Lines 1-7; *voice profile will be used for later voice verification*, [0018], Lines 10-11).

8. Regarding claim 6 and 23, Traynor discloses said biometric data input system is operable to obtain user biometric data from a user operating one of said plurality of extensions (*caller uses a wireless phone or wired telephone to enroll a voice profile*, [0018], Lines 1-7).

9. Regarding claim 7, Traynor discloses said security system is configurable through training to operate upon biometric data from said user (*authenticating the voice of a caller* and *caller's instructions directed to a remote appliance*, [0010], Lines 4-7).

10. Regarding claim 8, Traynor discloses said security system is configurable through training to operate upon biometric data from said user using training speech provided using said telephone system (*caller voice profile,* [0018]).

11. Regarding claim 9, Traynor discloses said security system includes direct interface for coupling to said secure resource (*wireline network connecting remote appliance to web server*, Fig. 1, element 410).

12. Regarding claim 10, Traynor discloses said direct interface is a wired connection to said secure resource (*wireline network connecting remote appliance to web server*, Fig. 1, element 410).

13. Regarding claim 11, Traynor discloses said direct interface is a network connection communicating with said secure resource (*wireline and wireless networks connecting the appliance network to the web server*, Fig. 1, elements 410 and 420).

14. Regarding claim 12, Traynor discloses said direct interface is a wireless connection communicating with said secure resource (*wireless network*, Fig. 1, element 420).

15. Regarding claim 13, Traynor discloses said biometric data input system is a voice input system ([0009], Lines 1-5).

16. Regarding claim 14, Traynor discloses said biometric input system is a voice input system communicating with said telephone through at least one of said extensions ([0009]; *speech recognition server* and *callers network*, Fig. 1, elements 110 and 200; *voice verification*, [0018], Lines 9-10).

17. Regarding claim 15, Traynor discloses said biometric verification/identification system employs a speaker verification/identification system (*voice verification*, [0018], Lines 9-10).

18. Regarding claim 17, Traynor discloses said biometric verification/identification system employs a speech recognition system that compares a text dependent component of said utterance with a predefined list of keywords (*user speaks appliance's*

label and voice is verified and query recognized, [0015], Lines 10-22; *Pepsi, Sprite, Gingerale*, [0015]).

19. Regarding claim 18, Traynor discloses said biometric verification/identification system employs a speech recognition system that employs a wordspotting system for identifying keywords within said utterance (*Pepsi, Sprite, Gingerale*, [0015]).

20. Regarding claim 19, Traynor discloses said biometric verification/identification system employs a speaker verification/identification system that assesses at least one text independent component and at least one text dependent component of said utterance (*voice profile, voice profile coupled with caller's own PIN* number, [0018]; *user speaks appliance's label and voice is verified and query recognized*, [0015], Lines 10-22; *Pepsi, Sprite, Gingerale*, [0015]).

21. Regarding claim 20, Traynor discloses said security server couples to said telephone system as one said plurality of extensions (*web server and wireline network*, Fig. 1, element 120).

22. Regarding claim 29, Traynor discloses storing biometric data associated with a plurality of users (*web server has callers' voice print*, [0019], Lines 8-9).

23. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Traynor (US Patent 2002/0007278), in view of Li *et al.* (US Patent 6,219,793).

24. Regarding claim 16 Traynor does not disclose but Li *et al.* do disclose said biometric verification/identification system automatically determines an extension identifier associated with said one of said plurality of extensions being operated by said user, and uses said extension identifier in accessing said stored biometric data (*caller ID and terminal ID are jointly authenticated*, Col. 16, Lines 16-18, 23-26 and 32-34; Col. 17, Lines 22-27 and 33-35).

Therefore it would have been obvious to one ordinarily skilled in the art at the time of the invention to supplement the teachings of Traynor with having said biometric verification/identification system automatically determine an extension identifier associated with said one of said plurality of extensions being operated by said user, and use said extension identifier in accessing said stored biometric data, as taught by Li *et al.*, in order to achieve a higher level of security in phone networks, as further taught by Li *et al.* (Col. 16, Lines 32-34).

25. Claims 21-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Traynor (US Patent 2002/0007278), in view of Hoskinson *et al.* (US Patent 5,339,351), and further in view of Li *et al.* (US Patent 6,219,793), further in view of Carter *et al.* ("An Integrated Biometric Database", IEE Colloquium on Electronic Images and Image Processing in Security and Forensic Sciences, IEE (1990)).

26. Regarding claim 21, Traynor discloses a method of interacting with a secure resource accessible through a telephone system of the type that provides telephone access through a plurality of extensions comprising the steps of:

receiving user biometric data from a user operating one of said extensions (*callers transmit voice through callers' network and a voice profile for each caller is developed,* [0018]);

evaluating said user biometric data vis-à-vis said stored biometric data (*application verifies caller's voice*, [0015], Lines 19-22; *voice profile will be used for voice verification*, [0018], Lines 10-11; *voice profile is coupled with caller's own pin number (two verification levels)*, [0018], Lines 12-13); and

providing instructions to interact with said secure resource based on the results of said evaluating step (*uses involving remote voice control of a system*, [0016], Lines 1-4).

However, Traynor does not explicitly disclose but Hoskinson *et al.* do disclose associating said plurality of extensions with a plurality of fixed physical locations (*location identification module associated with each extension*, see Abstract) and obtaining user extension information that identifies which one of said fixed physical locations the user is located (*location identification is enabled*, see Abstract).

Therefore it would have been obvious to one ordinarily skilled in the art at the time of the invention to supplement the teachings of Traynor with associating said plurality of extensions with a plurality of fixed physical locations and obtaining user extension information that identifies which one of said fixed physical locations the user

is located, as disclosed by Hoskinson *et al.*, in order to appropriately respond to a call based on the physical location of the caller.

Furthermore, the combined teachings of Traynor and Hoskinson *et al.* do not explicitly disclose but Li *et al.* do disclose using said user location information and said user biometric data to access a data store containing stored biometric data associated with stored extension information (*caller ID and terminal ID are jointly authenticated*, Col. 16, Lines 16-18, 23-26 and 32-34; Col. 17, Lines 22-27 and 33-35).

Therefore it would have been obvious to one ordinarily skilled in the art at the time of the invention to modify the combined teachings of Traynor and Hoskinson *et al.* by using said user location information and said user biometric data to access a data store containing stored biometric data associated with stored extension information, as taught by Li *et al.*, in order to effectively identify and verify a person making the call in conjunction with the identified location information to prevent fraud.

Moreover, the combined teachings of Traynor, Hoskinson *et al.* and Li *et al.* do not disclose but Carter *et al.* do disclose said verification/identification system is adapted to access a data structure storing associations among different types of biometric data and individual one of said extensions in order to retrieve stored biometric data associated with an extension being operated by a user (*see Integrated Database Overview, each subject record includes a voice recording, a signature record and a face image,* Page 2, 3rd Paragraph, Lines 1-8 and 12-22).

Therefore it would have been obvious to one ordinarily skilled in the art at the time of the invention to supplement the combined teachings of Traynor, Hoskinson *et al.*

and Li *et al.*, by having said verification/identification system be adapted to access a data structure storing associations among different types of biometric data associated and individual one of said extensions in order to retrieve stored biometric data associated with an extension being operated by a user, as taught by Carter *et al.*, in order to effectively retrieve the complete biometric record that corresponds to a particular user.

27. Regarding claim 22, Traynor discloses said biometric data is speech data (*voice verification*, [0018], Lines 9-12).

28. Regarding claim 23, Traynor discloses said biometric data is speech data provided through said one of said extensions (*callers' enrollment for voice verification, callers' network*, [0018]).

29. Regarding claim 24, Traynor discloses said evaluating step is performed using a speaker verification/identification technique applied to said speech data (*recognizing and authenticating*, [0010]; [0018]).

30. Regarding claim 25, Traynor discloses said biometric data is speech data and said evaluating step is performed using a speaker recognition to compare said speech data with a predefined set of keywords (*voice profile coupled with caller's own PIN number*, [0018], Lines 7-12; *Pepsi, Sprite, Gingerale*, [0015]).

31. Regarding claim 26, Traynor discloses said biometric data is stream of continuous speech data and said evaluating step is performed by wordspotting to identify keywords within said continuous speech data (*voice profile coupled with caller's own PIN number*, [0018], Lines 7-12; *Pepsi, Sprite, Gingerale*, [0015]).

32. Regarding claim 27, Traynor discloses said biometric data is stream of continuous speech data and said evaluating step is performed by assessing at least one text independent component and at least one text dependent component (*voice profile*, *voice profile coupled with caller's own PIN* number, [0018]; *user speaks appliance's label and voice is verified and query recognized*, [0015], Lines 10-22; *Pepsi, Sprite, Gingerale*, [0015]).

33. Claim 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over Traynor (US 2002/0007278), in view of Carter *et al.* ("An Integrated Biometric Database", IEE Colloquium on Electronic Images and Image Processing in Security and Forensic Sciences, IEE (1990)), further in view of Namba *et al.* (US Patent 5,884,249).

Regarding claim 30, the combined teachings of Traynor and Carter *et al.* do not Disclose but Namba *et al.* do disclose said apparatus is adapted to switch, in response to receipt of an utterance from said user from at least one of said extensions, from a manual entry mode to an automatic entry mode permitting hands-free gaining of access

by the user to the secure resource by providing only voice-based data entry, wherein said manual entry mode permits the user to gain access to the secure resource without automated, voice-based user authentication (*system is programmed to automatically switch between plural inputting means, including voice or manual operation, hence in order to switch from a manual operation mode to a voice mode the user changes the input mode to a voice one by inputting voice data*, Col. 5, Lines 21-26).

Therefore it would have been obvious to one ordinarily skilled in the art at the time of the invention to modify the combined teachings of Traynor and Carter *et al.* by having said apparatus be adapted to switch, in response to receipt of an utterance from said user from at least one of said extensions, from a manual entry mode to an automatic entry mode permitting hands-free gaining of access by the user to the secure resource by providing only voice-based data entry, wherein said manual entry mode permits the user to gain access to the secure resource without automated, voice-based user authentication, as disclosed by Namba *et al.*, in order to provide faster transition between imputing modes.

Conclusion

34. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Appel *et al.* (US 5,345,549) disclose a computer-based security system including a database of sensory data retrievable by multimedia-type cues.

35. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minerva Rivero whose telephone number is (571) 272-7626. The examiner can normally be reached on Monday-Friday 9:00 am - 6:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Wayne Young can be reached on (571) 272-7582. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MR 3/16/06

VIJAY CHAWAN
PRIMARY EXAMINER